Cyber Security and Energy: protecting the flow in a connected world

Cyber security is an increasingly hot topic in the energy industry. When it comes to infrastructure resilience and energy security, local and national governments are increasingly aware of the threats to critical assets and facilities posed by cyber attacks, whether criminal hackers, state-sponsored overseas agents or other bad actors.

In the era of the Internet of Things (IoT) when a domestic fridge might conceivably provide a back-door route to hack a mainframe, collaboration and information sharing between business and government are critical.

Energy underpins our society: its citizens, homes, public services and businesses. So imagine the potential impacts of cyber criminals targeting and interfering with critical national energy infrastructure—gas pipelines, power plants, nuclear facilities?

In a connected world, these assets are arguably more vulnerable to attack and disruption than ever before, with new technologies, energy systems and distribution networks compounding the risks. Digital systems are now fundamental to how electricity is generated, and to how electricity and gas are distributed. So how can we mitigate those risks?

In this complex, challenging and evolving area, it's vital that government and business work closely together to fully understand the issues faced, and to plan and implement the necessary protections and contingency plans to support energy security in an evolving cyber threat landscape. Here's an example of how this thinking is developing in the USA.

In spring 2019, industry players including the US Department of Energy (DOE), Federal Energy Regulatory Commission and the Electric Power Research Institute briefed the National Association of Regulatory Utility Commissioners Committee on Critical Infrastructure on the work they've been doing to protect energy infrastructure from both physical and cyber threats. The headline? *Energy infrastructure security requires continuous industry-government collaboration*. (***https://daily-energyinsider.com/featured/17597-energy-infrastructure-security-requires-continuous-industry-government-collaboration/***).

The US government only established its Office of Cybersecurity, Energy Security and Emergency Response (CESER) as recently as February 2018. Its priorities include better understanding the risks faced by the energy sector and how to manage and mitigate them. This includes clarifying the roles of industry and government in terms of cybersecurity, and building capacity in this area across industry and government.

At the DOE briefing, the president of the Edison Electric Institute (EEI), which represents all US investor-owned electric companies, said that companies are constantly working "to improve grid security, reliability, and resiliency, and we will continue to strengthen cyber and physical defences and to elevate preparedness. Our strong industry-government partnership… will continue to be key to accomplishing our shared goal of protecting the energy grid against all threats."

In the UK, collaboration is also seen as critical to success in the fast-changing cyber landscape. The Energy Emergencies Executive Committee (E3C) is a UK government committee run by the Department For Business, Energy & Industrial Strategy. It focuses on energy resilience and preparedness, advising government and ministers on plans, strategies and recommended responses. It also includes the Cyber Security Task Group (E3CC), whose members comprise the operating companies that run the UK's most critical national infrastructure for gas and electricity plus invited members from government, energy industry regulator Ofgem, and representatives from the UK's National Cyber Security Centre (NCSC).

In addition to performing risk assessments of the cyber threat, E3C is a way to share industry best practices, particularly relating to non-competitive issues and cyber security incidents of mutual concern. This kind of approach is critical, with the energy industry playing such an active and engaged role in moving the agenda forward.

If you don't know the work of the E3C, here's a good place to start. In August 2019, the UK experienced "a power disruption resulted from the operation of Low Frequency Demand Disconnection relays on the Great Britain power system… It impacted hundreds of thousands of customers, and caused significant secondary impacts in particular to the transport network. Though demand was fully restored within 90 minutes, the secondary impacts continued to be felt for much of the day." The E3C was commissioned to review this disruption, "to identify lessons and recommendations for the prevention and management of future power disruption events." This was not caused by a cyber attack, however the resulting disruption is something that might conceivably result from hacking with criminal intent. The key is building resilience; in this case, the E3C was tasked with identifying "areas of good practice and where improvements are required for system resilience" and making "recommendations for essential service resilience to power disruptions."

This is why organisations are now thinking about adding EV charging to their list of employee amenities. Unlike other 'softer' services or benefits, EV charging is something their people can use every day; a useful facility they'll appreciate is provided at their workplace. For employers, EV charging stations will be a useful addition to facilities aimed at attracting the brightest and the best employees while also supporting the organisation's green agenda. In this day and age, people increasingly want to work for businesses that take sustainability seriously.

The interim report was published in October 2019, and you can read it here - **https://www.gov.uk/government/publications/great-britain-power-system-disruption-review**.

Of course, no activity comes without some level of risk attached. You can never completely remove risk. But you can have plans in place to mitigate those risks, based on prior knowledge, domain expertise, current intelligence and the latest technologies. The public sector and businesses are doing just that, assessing the landscape and drawing up plans to thwart cyber attackers and protect their assets, to embed infrastructure resilience and therefore support a higher degree of energy security. The more we know and the more we collaborate, the stronger we are.

A world-class consulting partner for energy and utilities, Consultus was named **Most Trusted Consultancy (Large Customers)** *at the TELCA awards 2019.*

Contact information:

+44 (0)330 221 9899

info@consultus.com

the consultus international group